Historical Ciphers

Why (not) to study historical ciphers?

**AGAINST**
- Not similar to modern ciphers
- Long abandoned

**FOR**
- Basic components became a part of modern ciphers
- Under special circumstances modern ciphers reduce to historical ciphers
- Influence on world events
- The only ciphers you can break!
Secret Writing

Steganography
(hidden messages)

Cryptography
(encrypted messages)

Substitution Transformations

Codes
(replace words)

Substitution Ciphers
(replace letters)

Transposition Ciphers
(change the order of letters)

Selected world events affected by cryptology

1586 - trial of Mary Queen of Scots - substitution cipher

1917 - Zimmermann telegram, America enters World War I

1939-1945 Battle of England, Battle of Atlantic, D-day - ENIGMA machine cipher

1944 – world’s first computer, Colossus - German Lorenz machine cipher

1950s – operation Venona – breaking ciphers of soviet spies
stealing secrets of the U.S. atomic bomb
– one-time pad
### Ciphers used predominantly in the given period(1)

<table>
<thead>
<tr>
<th>Cryptography</th>
<th>Cryptanalysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 B.C.</td>
<td></td>
</tr>
<tr>
<td><strong>Shift ciphers</strong></td>
<td>Frequency analysis</td>
</tr>
<tr>
<td><strong>Monoalphabetic substitution cipher</strong></td>
<td>al-Kindi, Baghdad</td>
</tr>
<tr>
<td>1586 Invention of the Vigenère Cipher</td>
<td></td>
</tr>
<tr>
<td><strong>Homophonic ciphers</strong></td>
<td>Black chambers</td>
</tr>
<tr>
<td><strong>Vigenère cipher</strong></td>
<td></td>
</tr>
<tr>
<td>(Simple polyalphabetic substitution ciphers)</td>
<td>Kasiski’s method</td>
</tr>
<tr>
<td>1919 Invention of rotor machines</td>
<td>Index of coincidence</td>
</tr>
<tr>
<td><strong>Electromechanical machine ciphers</strong></td>
<td>William Friedman</td>
</tr>
<tr>
<td>(Complex polyalphabetic substitution ciphers)</td>
<td></td>
</tr>
<tr>
<td>1926 Vernam cipher (one-time pad)</td>
<td></td>
</tr>
</tbody>
</table>

### Ciphers used predominantly in the given period(2)

<table>
<thead>
<tr>
<th>Cryptography</th>
<th>Cryptanalysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1949 Shennon’s theory of secret systems</td>
<td>1932</td>
</tr>
<tr>
<td><strong>one-time pad</strong></td>
<td>Reconstructing ENIGMA</td>
</tr>
<tr>
<td><strong>Stream Ciphers</strong></td>
<td>Rejewski, Poland</td>
</tr>
<tr>
<td><strong>S-P networks</strong></td>
<td>Polish cryptological bombs,</td>
</tr>
<tr>
<td><strong>DES</strong></td>
<td>and perforated sheets</td>
</tr>
<tr>
<td>1977 Publication of DES</td>
<td>British cryptological bombs,</td>
</tr>
<tr>
<td></td>
<td>Bletchley Park, UK</td>
</tr>
<tr>
<td></td>
<td>Breaking Japanese</td>
</tr>
<tr>
<td></td>
<td>“Purple” cipher</td>
</tr>
<tr>
<td>2001</td>
<td>DES crackers</td>
</tr>
<tr>
<td></td>
<td>1990</td>
</tr>
<tr>
<td></td>
<td>1990</td>
</tr>
<tr>
<td></td>
<td>2001</td>
</tr>
</tbody>
</table>
Substitution Ciphers (1)

1. Monalphabetic (simple) substitution cipher

\[
M = m_1 \ m_2 \ m_3 \ m_4 \ \ldots \ \ m_N \\
C = f(m_1) \ f(m_2) \ f(m_3) \ f(m_4) \ \ldots \ f(m_N)
\]

Generally \( f \) is a random permutation, e.g.,

\[
f = \begin{bmatrix}
\text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{g} & \text{h} & \text{i} & \text{j} & \text{k} & \text{l} & \text{m} & \text{n} & \text{o} & \text{p} & \text{q} & \text{r} & \text{s} & \text{t} & \text{u} & \text{v} & \text{w} & \text{x} & \text{y} & \text{z}
\\
\text{s} & \text{l} & \text{t} & \text{a} & \text{v} & \text{m} & \text{c} & \text{e} & \text{r} & \text{u} & \text{b} & \text{q} & \text{p} & \text{d} & \text{f} & \text{k} & \text{h} & \text{w} & \text{y} & \text{g} & \text{x} & \text{z} & \text{j} & \text{n} & \text{i} & \text{o}
\end{bmatrix}
\]

Key = \( f \)

Number of keys = 26! \approx 4 \cdot 10^{26}

Monalphabetic substitution ciphers

Simplifications (1)

A. Caesar Cipher

\[
c_i = f(m_i) = m_i + 3 \mod 26
\]

\[
m_i = f^{-1}(c_i) = c_i - 3 \mod 26
\]

No key

B. Shift Cipher

\[
c_i = f(m_i) = m_i + k \mod 26
\]

\[
m_i = f^{-1}(c_i) = c_i - k \mod 26
\]

Key = \( k \)

Number of keys = 26
Caucasian Cipher: Example

Plaintext: I C A M E I S A W I C O N Q U E R E D
8 2 0 12 4 8 18 0 22 8 2 14 13 16 20 4 17 4 3
11 5 3 15 7 11 21 3 25 11 5 17 16 19 23 7 20 7 6
Ciphertext: L F D P H L V D Z L F R Q T X H U H G
Monalphabetic substitution ciphers
Simplifications (2)

C. Affine Cipher

\[ c_i = f(m_i) = k_1 \cdot m_i + k_2 \mod 26 \]
\[ \gcd(k_1, 26) = 1 \]

\[ m_i = f^{-1}(c_i) = k_1^{-1} \cdot (c_i - k_2) \mod 26 \]

Key = \((k_1, k_2)\)
Number of keys = \(12 \cdot 26 = 312\)

Most frequent single letters

*Average frequency in a random string of letters:*

\[ \frac{1}{26} = 0.038 = 3.8\% \]

*Average frequency in a long English text:*

<table>
<thead>
<tr>
<th>Letter</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>13%</td>
</tr>
<tr>
<td>T, N, R, I, O, A, S</td>
<td>6%-9%</td>
</tr>
<tr>
<td>D, H, L</td>
<td>3.5%-4.5%</td>
</tr>
<tr>
<td>C, F, P, U, M, Y, G, W, V</td>
<td>1.5%-3%</td>
</tr>
<tr>
<td>B, X, K, Q, J, Z</td>
<td>&lt; 1%</td>
</tr>
</tbody>
</table>
Most frequent digrams, and trigrams

**Digrams:**

TH, HE, IN, ER, RE, AN, ON, EN, AT

**Trigrams:**

THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Relative frequency of letters in a long English text

*by Stallings*

<table>
<thead>
<tr>
<th>Letter</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>8.5</td>
</tr>
<tr>
<td>B</td>
<td>7.25</td>
</tr>
<tr>
<td>C</td>
<td>0.25</td>
</tr>
<tr>
<td>D</td>
<td>0.5</td>
</tr>
<tr>
<td>E</td>
<td>12.75</td>
</tr>
<tr>
<td>F</td>
<td>2.25</td>
</tr>
<tr>
<td>G</td>
<td>1.5</td>
</tr>
<tr>
<td>H</td>
<td>1.5</td>
</tr>
<tr>
<td>I</td>
<td>3.75</td>
</tr>
<tr>
<td>J</td>
<td>0.5</td>
</tr>
<tr>
<td>K</td>
<td>7.75</td>
</tr>
<tr>
<td>L</td>
<td>7.75</td>
</tr>
<tr>
<td>M</td>
<td>7.5</td>
</tr>
<tr>
<td>N</td>
<td>7.5</td>
</tr>
<tr>
<td>O</td>
<td>2.75</td>
</tr>
<tr>
<td>P</td>
<td>0.5</td>
</tr>
<tr>
<td>Q</td>
<td>2.75</td>
</tr>
<tr>
<td>R</td>
<td>6</td>
</tr>
<tr>
<td>S</td>
<td>9.25</td>
</tr>
<tr>
<td>T</td>
<td>3.75</td>
</tr>
<tr>
<td>U</td>
<td>3</td>
</tr>
<tr>
<td>V</td>
<td>2.75</td>
</tr>
<tr>
<td>W</td>
<td>1.5</td>
</tr>
<tr>
<td>X</td>
<td>1.5</td>
</tr>
<tr>
<td>Y</td>
<td>0.5</td>
</tr>
<tr>
<td>Z</td>
<td>0.25</td>
</tr>
</tbody>
</table>
Character frequency in a long English plaintext

Character frequency in the corresponding ciphertext for a shift cipher

Character frequency in a long English plaintext

Character frequency in the corresponding ciphertext for a general monoalphabetic substitution cipher
**Frequency analysis attack: relevant frequencies**

<table>
<thead>
<tr>
<th></th>
<th>Frequency Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Frequency analysis attack (1)**

**Step 1:** Establishing the relative frequency of letters in the ciphertext

**Ciphertext:**

```
FMXVE DKAPH FERBN DKRXR SREFM ORUDS
DKDVS HVUFE DKAPR KDLYE VLRHH RH
```

**Frequency Distribution:**

```
R    - 8
D    - 7
E, H, K    - 5
```
Frequency analysis attack (2)

Step 2: Assuming the relative frequency of letters in the corresponding message, and deriving the corresponding equations

Assumption: Most frequent letters in the message: E and T

Corresponding equations:

\[
\begin{align*}
E & \rightarrow R \quad f(E) = R \\
T & \rightarrow D \quad f(T) = D \\
4 & \rightarrow 17 \quad f(4) = 17 \\
19 & \rightarrow 3 \quad f(19) = 3
\end{align*}
\]

Frequency analysis attack (3)

Step 3: Verifying the assumption for the case of affine cipher

\[
\begin{align*}
f(4) & = 17 \\
f(19) & = 3
\end{align*}
\]

\[
\begin{align*}
4k_1 + k_2 & \equiv 17 \pmod{26} \\
19k_1 + k_2 & \equiv 3 \pmod{26}
\end{align*}
\]

\[
\begin{align*}
15k_1 & \equiv -14 \pmod{26} \\
15k_1 & \equiv 12 \pmod{26}
\end{align*}
\]
Substitution Ciphers (2)

2. Polyalphabetic substitution cipher

\[ M = \begin{array}{cccc}
  m_1 & m_2 & \ldots & m_d \\
  m_{d+1} & m_{d+2} & \ldots & m_{2d} \\
  m_{2d+1} & m_{2d+2} & \ldots & m_{3d}
\end{array} \]

\[ C = \begin{array}{cccc}
  f_1(m_1) & f_2(m_2) & \ldots & f_d(m_d) \\
  f_1(m_{d+1}) & f_2(m_{d+2}) & \ldots & f_d(m_{2d}) \\
  f_1(m_{2d+1}) & f_2(m_{2d+2}) & \ldots & f_d(m_{3d})
\end{array} \]

\[ \ldots \]

\[ d \text{ is a period of the cipher} \]

Key = d, f_1, f_2, \ldots, f_d

Number of keys for a given period \( d = (26!)^d \approx (4 \cdot 10^{26})^d \)
Polyalphabetic substitution ciphers
Simplifications (1)

A. Vigenère cipher: polyalphabetic shift cipher
Invented in 1568

\[ c_i = f_{i \mod d}(m_i) = m_i + k_{i \mod d} \mod 26 \]

\[ m_i = f_{i \mod d}^{-1}(c_i) = m_i - k_{i \mod d} \mod 26 \]

Key = \( k_0, k_1, \ldots, k_{d-1} \)

Number of keys for a given period \( d = (26)^d \)

Vigenère Square

plaintext:

```
plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z
```

<table>
<thead>
<tr>
<th>Key = “nsa”</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>
**Vigenère Cipher - Example**

**Plaintext:**  
TO BE OR NOT TO BE  

**Key:**  
NSA  

**Encryption:**  

<table>
<thead>
<tr>
<th>TOB</th>
<th>EOR</th>
<th>NOT</th>
<th>TOB</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>GGB</td>
<td>RGR</td>
<td>AGR</td>
<td>GGB</td>
<td>R</td>
</tr>
</tbody>
</table>

**Ciphertext:** GGBRGRAGTGGGR

---

**Determining the period of the polyalphabetic cipher**  
**Kasiski’s method**

**Ciphertext:**  

\[ \underline{G G B R G R A G T G G B R} \]

Distance = 9

*Period \(d\) is a divisor of the distance between identical blocks of the ciphertext*

- In our example: \(d = 3\) or 9
**Index of coincidence method (1)**

$n_i$ - number of occurrences of the letter $i$ in the ciphertext

$i = a \ldots z$

$N$ - length of the ciphertext

$p_i = \text{frequency of the letter } i \text{ for a long ciphertext}$

$$p_i = \lim_{N \to \infty} \frac{n_i}{N}$$

$$\sum_{i=a}^{z} p_i = 1$$

**Index of coincidence method (2)**

Measure of roughness:

$$M.R. = \sum_{i=a}^{z} \left( p_i - \frac{1}{26} \right)^2 = \sum_{i=a}^{z} p_i^2 - \frac{1}{26}$$

<table>
<thead>
<tr>
<th>Period</th>
<th>0.028</th>
<th>0.014</th>
<th>0.006</th>
<th>0.003</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.028</td>
<td>0.014</td>
<td>0.006</td>
<td>0.003</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>
Index of coincidence method (3)

Index of coincidence

The approximation of \( \sum_{i=a}^{z} p_i^2 \)

Definition:

Probability that two random elements of the ciphertext are identical

Formula:

\[
I.C. = \sum_{i=a}^{z} \frac{n_i}{N} = \sum_{i=a}^{z} \frac{(n_i-1) \cdot n_i}{(N-1) \cdot N}
\]

Index of coincidence method (4)

Measure of roughness

\[
M.R. = I.C. - \frac{1}{26} = \sum_{i=a}^{z} \frac{(n_i-1) \cdot n_i}{(N-1) \cdot N} - \frac{1}{26}
\]

<table>
<thead>
<tr>
<th>period</th>
<th>M.R.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.028</td>
</tr>
<tr>
<td>2</td>
<td>0.014</td>
</tr>
<tr>
<td>5</td>
<td>0.006</td>
</tr>
<tr>
<td>10</td>
<td>0.003</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>period</th>
<th>M.R.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.028</td>
</tr>
<tr>
<td>2</td>
<td>0.014</td>
</tr>
<tr>
<td>5</td>
<td>0.006</td>
</tr>
<tr>
<td>10</td>
<td>0.003</td>
</tr>
</tbody>
</table>
Polyalphabetic substitution ciphers
Simplifications (2)

B. Rotor machines used before and during the WWII

<table>
<thead>
<tr>
<th>Country</th>
<th>Machine</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany:</td>
<td>Enigma</td>
<td>(d=26 \cdot 25 \cdot 26 = 16,900)</td>
</tr>
<tr>
<td>U.S.A.:</td>
<td>M-325, Hagelin M-209</td>
<td></td>
</tr>
<tr>
<td>Japan:</td>
<td>“Purple”</td>
<td></td>
</tr>
<tr>
<td>UK:</td>
<td>Typex</td>
<td>(d=26 \cdot (26-k) \cdot 26, k=5, 7, 9)</td>
</tr>
<tr>
<td>Poland:</td>
<td>Lacida</td>
<td>(d=24 \cdot 31 \cdot 35 = 26,040)</td>
</tr>
</tbody>
</table>

Substitution Ciphers (3)

3. Running-key cipher

\[
M = m_1 \quad m_2 \quad m_3 \quad m_4 \quad \ldots \quad m_N \\
K = k_1 \quad k_2 \quad k_3 \quad k_4 \quad \ldots \quad k_N
\]

**K is a fragment of a book**

\[
C = c_1 \quad c_2 \quad c_3 \quad c_4 \quad \ldots \quad c_N
\]

\[
c_i = m_i + k_i \mod 26 \\
m_i = c_i - k_i \mod 26
\]

**Key:** book (title, edition), position in the book (page, row)
Substitution Ciphers (4)

4. Polygram substitution cipher

\[ M = \begin{array}{cccc}
    m_1 & m_2 & \ldots & m_d \\
    m_{d+1} & m_{d+2} & \ldots & m_{2d} \\
    m_{2d+1} & m_{2d+2} & \ldots & m_{3d} \\
\end{array} - M_1 \\
\begin{array}{cccc}
    M_2 \\
    M_3 \\
\end{array} \]

\[ C = \begin{array}{cccc}
    c_1 & c_2 & \ldots & c_d \\
    c_{d+1} & c_{d+2} & \ldots & c_{2d} \\
    c_{2d+1} & c_{2d+2} & \ldots & c_{3d} \\
\end{array} - C_1 \\
\begin{array}{cccc}
    C_2 \\
    C_3 \\
\end{array} \]

\[ \begin{array}{c}
    \ldots \\
    \ldots \\
\end{array} \]

\[ d \text{ is the length of a message block} \]

\[ C_i = f(M_i) \quad M_i = f^1(C_i) \]

Key = d, f

Number of keys for a given block length \( d = (26^d)! \)
Playfair Cipher

Key:

PLAYFAIR IS A DIGRAM CIPHER

\[
\begin{array}{c|c|c|c|c}
P & L & A & Y & F \\
\hline
I & R & S & D & G \\
M & C & H & E & B \\
K & N & O & Q & T \\
U & V & W & X & Z \\
\end{array}
\]

Convetion 1

message P O L A N D  
ciphertext A K A Y Q R 

Convetion 2

message P O L A N D  
ciphertext K A R S R Q 

Hill Cipher

Ciphering:

\[
C_{1\times d} = M_{1\times d} \cdot K_{d\times d}
\]

\[
(c_1, c_2, \ldots, c_d) = (m_1, m_2, \ldots, m_d) \\
\begin{pmatrix}
k_{11}, k_{12}, \ldots, k_{1d} \\
k_{d1}, k_{d2}, \ldots, k_{dd}
\end{pmatrix}
\]

ciphertext block = message block \cdot key matrix
Hill Cipher

Deciphering:

\[ M_{[1 \times d]} = C_{[1 \times d]} \cdot K^{-1}_{[d \times d]} \]

message block = ciphertext block \cdot inverse key matrix

where

\[
K_{[d \times d]} \cdot K^{-1}_{[d \times d]} =
\begin{pmatrix}
1, 0, \ldots, 0, 0 \\
0, 1, \ldots, 0, 0 \\
\vdots \\
0, 0, \ldots, 1, 0 \\
0, 0, \ldots, 0, 1
\end{pmatrix}
\]

key matrix \cdot inverse key matrix = identity matrix

Hill Cipher - Known Plaintext Attack (1)

Known:

\[
\begin{align*}
C_1 &= (c_{11}, c_{12}, \ldots, c_{1d}) & M_1 &= (m_{11}, m_{12}, \ldots, m_{1d}) \\
C_2 &= (c_{21}, c_{22}, \ldots, c_{2d}) & M_2 &= (m_{21}, m_{22}, \ldots, m_{2d}) \\
& \vdots & \vdots & \vdots \\
C_d &= (c_{d1}, c_{d2}, \ldots, c_{dd}) & M_d &= (m_{d1}, m_{d2}, \ldots, m_{dd})
\end{align*}
\]

We know that:

\[
\begin{align*}
(c_{11}, c_{12}, \ldots, c_{1d}) &= (m_{11}, m_{12}, \ldots, m_{1d}) \cdot K_{[d \times d]} \\
(c_{21}, c_{22}, \ldots, c_{2d}) &= (m_{21}, m_{22}, \ldots, m_{2d}) \cdot K_{[d \times d]} \\
& \vdots \vdots \vdots \\
(c_{d1}, c_{d2}, \ldots, c_{dd}) &= (m_{d1}, m_{d2}, \ldots, m_{dd}) \cdot K_{[d \times d]}
\end{align*}
\]
Hill Cipher - Known Plaintext Attack (2)

\[
\begin{pmatrix}
c_{11}, c_{12}, \ldots, c_{1d} \\
c_{21}, c_{22}, \ldots, c_{2d} \\
\cdots \cdots \cdots \\
c_{d1}, c_{d2}, \ldots, c_{dd}
\end{pmatrix}
= \begin{pmatrix}
m_{11}, m_{12}, \ldots, m_{1d} \\
m_{21}, m_{22}, \ldots, m_{2d} \\
\cdots \cdots \cdots \\
m_{d1}, m_{d2}, \ldots, m_{dd}
\end{pmatrix}
= \begin{pmatrix}
k_{11}, k_{12}, \ldots, k_{1d} \\
k_{21}, k_{22}, \ldots, k_{2d} \\
\cdots \cdots \cdots \\
k_{d1}, k_{d2}, \ldots, k_{dd}
\end{pmatrix}
\]

\[
C_{[d \times d]} = M_{[d \times d]} \cdot K_{[d \times d]}
\]

\[
K_{[d \times d]} = M^{-1}_{[d \times d]} \cdot C_{[d \times d]}
\]

Substitution Ciphers (5)

4. Homophonic substitution cipher

\( M = \{ \text{A, B, C, …, Z} \} \)
\( C = \{ \text{0, 1, 2, 3, …, 99} \} \)

\( c_i = f(m_i, \text{random number}) \)
\( m_i = f^{-1}(c_i) \)

\( f: \)
\( E \rightarrow 17, 19, 27, 48, 64 \)
\( A \rightarrow 8, 20, 25, 49 \)
\( U \rightarrow 45, 68, 91 \)
\( \ldots \)
\( X \rightarrow 33 \)
Transposition ciphers

\[ M = m_1 \ m_2 \ m_3 \ m_4 \ \ldots \ \ m_N \]
\[ C = m_{f(1)} \ m_{f(2)} \ m_{f(3)} \ m_{f(4)} \ \ldots \ \ m_{f(N)} \]

Letters of the plaintext are rearranged without changing them
### Transposition cipher

**Example**

| Plaintext: | CRYPTANALYST |
| Key: | KRIS |
| Encryption: | KRIS
| | CYRNP
| | TANAL
| | LYST |

| Ciphertext: | YNSCTRLAYPAT |

### One-time Pad

**Vernam Cipher**

*Gilbert Vernam, AT&T*  
*Major Joseph Mauborgne*  
*1926*

\[ c_i = m_i \oplus k_i \]

|  |  |
|---|---|---|---|---|
| \( m_i \) | 0111011010100101011010110110101 |
| \( k_i \) | 1101110111011001011101101100110 |
| \( c_i \) | 10101011011111111000011 |

*All bits of the key must be chosen at random and never reused*
One-time Pad
Equivalent version

\[ c_i = m_i + k_i \mod 26 \]

| \( m_i \) | TO BE OR NOT TO BE |
| \( k_i \) | AX TC VI URD WM OF |
| \( c_i \) | TL UG JZ HFW PK PJ |

All letters of the key must be chosen at random and never reused.

Perfect Cipher

*Claude Shannon*

*Communication Theory of Secrecy Systems, 1948*

\[ \forall \quad P(M=m \mid C=c) = P(M = m) \]

\( m \in M \)

\( c \in C \)

The cryptanalyst can guess a message with the same probability without knowing a ciphertext as with the knowledge of the ciphertext.
Is substitution cipher a perfect cipher?

\[ C = XRZ \]

\[ P(M=ADD \mid C=XRZ) = 0 \]

\[ P(M=ADD) \neq 0 \]

Is one-time pad a perfect cipher?

\[ C = XRZ \]

\[ P(M=ADD \mid C=XRZ) \neq 0 \]

\[ P(M=ADD) \neq 0 \]

M might be equal to

\[ CAT, PET, SET, ADD, BBC, AAA, HOT, HIS, HER, BET, WAS, NOW, \text{ etc.} \]
S-P Networks

Basic operations of S-P networks

Substitution

Permutation

S-box

P-box
Avalanche effect

LUCIFER

Horst Feistel, Walt Tuchman
IBM

16 rounds
LUCIFER- external look

plaintext block

128 bits

LUCIFER

key

512 bits

128 bits

ciphertext block